Claims

1. A device, located at a remote site on a network having a plurality of remote sites, for validating the source of an information item transmitted over said network, said device comprising:

a processor in communication with a memory, said processor operable to execute code for:

determining a first comparator value in relation to a first value associated with said information item received over said network and a Diffie-Hellman public key;

determining a second comparator value in relation to a digital signature received, said digital signature determined in association with a second value associated with said information item prior to transmission over said network; and

comparing said first and second comparator values and validating said source based on said comparison.

2. The device as recited in claim 1, wherein said processor is further operable to execute code for determining said first value as a hash value of said received information items.

3. The device as recited in claim 1, wherein said public key is in the form of

$$g^{xz} \bmod(n)$$

wherein g, x, z, and n are randomly selected large numbers and n is a prime number.

4. The device as recited in claim 3, wherein said public key is selected from the group consisting of: known, preloaded, pre-determined, determinable.

5. The device as recited in claim 3, wherein said processor is operable to read said public key from an external media consisting of: magnetic tape, optic, memory.

6. The device as recited in claim 3, wherein said processor is operable to execute code for receiving selected ones of said randomly selected large numbers over said network.

7. The device as recited in claim 1, wherein said processor is further operable to execute code for receiving said public key over said network.

8. The device as recited in claim 3, wherein said processor is further operable to obtain selected ones of said randomly selected large numbers from preloaded sources from the group consisting of: magnetic tape, optic medium, memory.

9. The device as recited in claim 1, further comprising:

an I/O unit in communication with said processor and said network.

10. The device as recited in claim 9, wherein said I/O unit is further in communication with said memory.

11. The device as recited in claim 1, wherein said code is stored in said memory.

12. The device as recited in claim 1, wherein said second value is a hash value.

13. The device as recited in claim 1, wherein said source is validated when said first and second comparator values are equal.

14. A method for validating the source of an information item transmitted over a network, said method comprising the steps of:

determining a first comparator value in relation to a first value associated with said information item transmitted over said network and a Diffie-Hellman public key;

determining a second comparator value in relation to a digital signature, wherein said digital signature is associated with said information items prior to transmission over said network; and

comparing said first and second comparator values and validating said source based on said comparison.

15. The method as recited in claim 14, further comprising the step of:

determining said first value as a hash value of said information items.

16. The method as recited in claim 14, wherein said public key is in the form of:

$$g^{xz} \bmod(n)$$

wherein g, x, z, and n are said randomly selected large numbers and n is a prime number.

17. The method as recited in claim 16, wherein said pubic key is selected from the group consisting of: known, preloaded, predetermined, determinable.

18. The method as recited in claim 16, wherein said public key is transmitted over said network.

19. The method as recited in claim 16, wherein selected ones of said large number values are selected from the group consisting of: known, preloaded, predetermined.

20. The method as recited in claim 16, wherein selected ones of said large number values are received from said network.

21. The method as recited in claim 14, wherein said source is validated when said first and second comparator values are equal.

22. A device for generating digital signatures comprising:

a processor in communication with a memory, said processor operable to execute code for:

generating a first and second Diffie-Hellman public key from a plurality of large numbers randomly selected, wherein at least one of said numbers is a prime number; and

determining a public key as a Diffie-Hellman transpose of one of said Diffie-Hellman public keys.

23. The device as recited in claim 22, further comprising:

a device in communication with said processor, said device operable to transmit said public key and a remaining one of said Diffie-Hellman public keys to an external device.

24. The device as recited in claim 23, wherein said external device is selected from the group consisting of: a network, a magnetic medium, an optical medium, human-readable media.